SECURITY FEATURES IN HPE PROLIANT GEN10 SERVERS CASE STUDY

Large Enterprise Insurance Company

Introduction

This case study of a large enterprise insurance company is based on an August 2018 survey of security features in HPE ProLiant Gen10 servers customers by TechValidate, a 3rd-party research service. The profiled company asked to have their name blinded to protect their confidentiality.

> "With the new security features of HPE ProLiant Gen10 servers, we feel safer than before."

Challenges

The business challenges that led the profiled company to evaluate and ultimately select security features in HPE ProLiant Gen10 servers:

- Addressed the following security challenges with the security features in HPE Gen10 ProLiant servers:
  - Validate that their server was free of malware prior to arrival at their facility
  - Check for compromised server firmware at runtime without rebooting
  - Automatically remove malware and recover their servers at extreme scale (thousands) back to an operational state

Use Case

The key features and functionalities of security features in HPE ProLiant Gen10 servers that the surveyed company uses:

- Running the following workloads/applications on their HPE ProLiant Gen10 servers to aid their security concerns:
  - Virtual Desktop Infrastructure applications

Results

The surveyed company achieved the following results with security features in HPE ProLiant Gen10 servers:

- Believes that HPE ProLiant Gen10 servers are superior to/better than similar servers in the market because:
  - The 24 hour detection capabilities through Run Time Firmware Verification give them peace of mind knowing that their HPE servers are secure and checked regularly
  - Their HPE servers can recover quickly back to a safe operational state after a ransomware event
  - They are confident that servers arrive from production to their facility with no tampering
  - They are immediately notified of any malware or compromised code in server essential firmware through my iLO logs
- Rates the value of the security capabilities offered on HPE ProLiant Gen10 servers:
  - immutable fingerprint in the HPE silicon that ensures Gen10 servers cannot boot compromised code: valuable
  - ability to check the integrity of essential firmware before it is executed: very valuable
  - ability to check the integrity of essential firmware while the server is up and running: very valuable
  - support for high-grade Commercial National Security Algorithm (CNSA) for encryption renumber: valuable
  - ability to automatically recover essential server firmware: valuable
  - ability to recover firmware at scale (up to 10,000 servers in one click): valuable
  - ability to recover host environment, operating system, applications and firmware settings: valuable
  - assurance that their servers are equipped with National Institute of Standards & Technology (NIST) 800-53 Controls: very valuable
- Rates their confidence in defending their server against malware attacks with HPE ProLiant Gen10 servers:
  - protecting their server against a malware attack: very confident
  - detecting a malware attack on their server: confident
  - recovering from a malware attack on their server: confident
- Rates the time spent doing the tasks needed to secure their server from firmware attacks:
  - before /without Proliant Gen10: ~ 1 hour to 1 day
  - after Proliant Gen10: less than an hour
- Saw improvements in the time required for the following tasks since using HPE ProLiant Gen10 security features:
  - time needed to conduct daily server firmware validation checks: >50%
  - time needed to recover from a malware attack: >50%
  - time to scale recovery to thousands of servers back to their operational state in a single click: 26 – 50%
  - time to ensure compliance with security audits: >50%

Company Profile

The company featured in this case study asked to have its name publicly blinded because publicly endorsing vendors is against their policies.

TechValidate stands behind the authenticity of this data.

Company Size:
Large Enterprise

Industry:
Insurance

Source: TechValidate survey of a Large Enterprise Insurance Company

Research by TechValidate by SurveyMonkey

Validated Published: Sep. 10, 2018 TVID: 0FD-F3F-088